

AMENDMENTS TO THE CLAIMS

1. (original) A method for automatically negotiating a security protocol, comprising:

receiving a security authorization request to establish a secure connection

between an internal node, the internal node being internal to a security-enabled domain, and an external node, the external node being external to the security-enabled domain;

comparing a first protocol set associated with the internal node to a second protocol set associated with the external node; and

establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and the second protocol set is found.
2. (original) A method according to claim 1, wherein the external node comprises at least one of a computer and a network-enabled wireless device.
3. (original) A method according to claim 1, wherein the internal node comprises at least one of a client computer and a server.
4. (original) A method according to claim 1, wherein the security-enabled domain comprises a distributed directory domain.
5. (original) A method according to claim 1, wherein the security-enabled domain comprises a certificate-based domain.

6. (original) A method according to claim 5, wherein the certificate-based domain comprises a Kerberos-enabled domain.

7. (original) A method according to claim 6, wherein the matching protocol comprises an X.509 certificate.

8. (original) A method according to claim 1, wherein the security authorization request is generated by the external node.

9. (original) A method according to claim 8, wherein the step of receiving the security authorization request is executed by the internal node.

10. (original) A method according to claim 1, wherein the security authorization request is generated by the internal node.

11. (original) A method according to claim 10, wherein the step of receiving the security authorization request is executed by the external node.

12. (original) A method according to claim 1, further comprising a step of terminating the secure connection when a session between the external node and the internal node is complete.

13. (original) A method according to claim 1, further comprising a step of terminating connection processing when no match between the first protocol set and the second protocol set is found.

14. (original) A method according to claim 1, further comprising a step of selecting a protocol to use in establishing the secure connection when a plurality of matching protocols are found.

15. (original) A method according to claim 1, further comprising a step of authenticating at least one of the internal node and the external node.

16. (original) A method according to claim 15, wherein the step of authenticating comprises communicating a certificate to a certificate authority.

17. (currently amended) A system for automatically negotiating a security protocol, comprising:

~~a first interface to an internal node, the internal node being internal to a security-enabled domain, the internal node having an associated first protocol set; and~~

~~a second interface to an external node, the external node being external to the security-enabled domain, the external node having an associated second protocol set; and~~

a negotiation engine, the negotiation engine receiving a security authorization request to establish a secure connection between the internal node and ~~[[the]]~~ an external node being external to the security-enabled domain and having an associated second protocol set, comparing the first protocol set associated with the internal node to the second protocol set associated with the external node, and establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and the second protocol set is found.

18. (original) A system according to claim 17, wherein the external node comprises at least one of a computer and a network-enabled wireless device.

19. (original) A system according to claim 17, wherein the internal node comprises at least one of a client computer and a server.

20. (original) A system according to claim 17, wherein the security-enabled domain comprises a distributed directory domain.

21. (original) A system according to claim 17, wherein the security-enabled domain comprises a certificate-based domain.

22. (original) A system according to claim 21, wherein the certificate-based domain comprises a Kerberos-enabled domain.

23. (original) A system according to claim 22, wherein the matching protocol comprises an X.509 certificate.

24. (original) A system according to claim 17, wherein the security authorization request is generated by the external node.

25. (original) A system according to claim 24, wherein the security authorization request is received by the internal node.

26. (original) A system according to claim 17, wherein the security authorization request is generated by the internal node.

27. (original) A system according to claim 26, wherein the security authorization request is received by the external node.

28. (original) A system according to claim 17, wherein the negotiation engine terminates the secure connection when a session between the external node and the internal node is complete.

29. (original) A system according to claim 17, wherein the negotiation engine terminates connection processing when no match between the first protocol set and the second protocol set is found.

30. (original) A system according to claim 17, wherein the negotiation engine selects a protocol to use in establishing the secure connection when a plurality of matching protocols are found.

31. (original) A system according to claim 17, wherein at least one of the internal node and the external node authenticates the other.

32. (original) A system according to claim 31, wherein the authenticating comprises communicating a certificate to a certificate authority.

33-48. (cancelled)

49. (currently amended) One or more tangible computer-readable media having computer-executable instructions embodied thereon ~~A computer-readable medium, the computer readable medium~~ computer-executable instructions being readable configured to execute a method for automatically negotiating a security protocol, the method comprising:

receiving a security authorization request to establish a secure connection between an internal node, the internal node being internal to a security-enabled domain, and an external node, the external node being external to the security-enabled domain;

comparing a first protocol set associated with the internal node to a second protocol set associated with the external node; and

establishing a secure connection between the external node and the internal node when a matching protocol between the first protocol set and the second protocol set is found.

50. (currently amended) ~~A computer-readable medium according to The one or more computer-readable media of claim 49, wherein the external node comprises at least one of a computer and a network-enabled wireless device.~~

51. (currently amended) ~~A computer-readable medium according to The one or more computer-readable media of claim 49, wherein the internal node comprises at least one of a client computer and a server.~~

52. (currently amended) ~~A computer-readable medium according to The one or more computer-readable media of claim 49, wherein the security-enabled domain comprises a distributed directory domain.~~

53. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 49, wherein the security-enabled domain comprises a certificate-based domain.

54. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 53, wherein the certificate-based domain comprises a Kerberos-enabled domain.

55. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 54, wherein the matching protocol comprises an X.509 certificate.

56. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 49, wherein the step of generating a security authorization request is executed by the external node.

57. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 56, wherein the step of receiving the security authorization request is executed by the internal node.

58. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 49, wherein the step of generating a security authorization request is executed by the internal node.

59. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 58, wherein the step of receiving the security authorization request is executed by the external node.

60. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 49, wherein the method further comprises a step of terminating the secure connection when a session between the external node and the internal node is complete.

61. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 49, wherein the method further comprises a step of terminating connection processing when no match between the first protocol set and the second protocol set is found.

62. (currently amended) ~~A computer-readable medium according to~~ The one or more computer-readable media of claim 49, wherein the method further comprises a step of selecting a protocol to use in establishing the secure connection when a plurality of matching protocols are found.